DM 380-1-8

DEPARTMENT OF THE ARMY
Corps of Engineers, Omaha District
215 North 17th Street
Omaha Nebraska 68102-4978

CEMRO-IM/CEMRO-SE

Memorandum
No. 380-1-8

15 December 1992

Security
INFORMATION MANAGEMENT (IM) SECURITY PLAN

1. Purpose. To implement security in accordance with (IAW) AR 380-19 within the Omaha District.

2. Applicability. This memorandum is applicable to all elements of the Omaha District.

3. Reference.

a. AR 380-19

b. DM 25-1-1

4. Objectives. The objective of the Information Management (IM) Security Plan is to:

a. Define responsibilities of the Information System Security Manager (ISSM), Information System Security Officer (ISSO), Network Security Officer (NSO), Terminal Area Security Officers (TASO), Chief Information Management (CIM), division chiefs, and computer resource users.

b. Define the procedure for password issuance.

c. Define minimum requirements for security marking and disposal of mainframe generated products.

d. Describe the procedure for microcomputer accreditation requests.

e. Describe minimum acceptable security training requirements.

f. Define minimum acceptable standards for the protection of data, hardware and software.

g. Define policy on IM resources as it applies to waste, fraud and abuse.

This memorandum supersedes DM 380-1-8, dated 24 February 1986.

5. Responsibilities.

a. The Commander will:

(1) Ensure fullest integration and coordination of activities in support of the security requirements of both assigned and tenant data processing activities (DPA's)/telecommunications automated information systems (TAIS).

(2) Appoint an installation ISSM to act as the focal point for all information system security matters.

(3) Appoint an ISSO to act as the point of contact for all technical implementation and monitoring of IM security for all Omaha District IM assets.

(4) Function as the accreditation authority for those systems designated as class sensitive 3 (CS3) and unclassified sensitive 1 (US1).

(5) Ensure that each site handling sensitive defense information implements an effective risk management program.

(6) Serve as accreditation authority for sensitive accreditation and final reviewer of statements of nonsensitivity.

b. The Information System Security Manager (ISSM) will:

(1) Be responsible for implementing and maintaining the IM security plan.

(2) Act as the focal point for and principle adviser to the District Commander on information systems security matters.

(3) Formally designate each individual who has been assigned a computer userid with the appropriate sensitivity designation and determine their suitability for continued employment.

(4) Develop a facility security profile (FSP) as defined by AR 380-19, Chapter 2, Section IV, which would include a list of all data terminals and microcomputers in the Omaha District, their physical location, and the individual who has been assigned responsibility for the terminal.

(5) Ensure that automation security actions of the ISSO, NSO and TASO are integrated.

(6) Ensure that the ISSO and NSO receive adequate support for their information security requirements, to include receiving assistance during the accreditation process to ensure that all threats have been identified and vulnerabilities addressed.

(7) Ensure that all passwords for Corps of Engineers Automated Processing (CEAP) systems are issued using the UPASS process. (See para. 6.)

(8) Maintain an accurate roster of the responsible ISSO, NSO and TASO.

(9) Maintain accurate records of all security incidents involving information systems, ensure adequate investigations IAW AR 380-19, para 2-28, and analyze such incidents for trend indication.

(10) Advise the CIM of available U.S. Army Intelligence and Security Command information security services. The ISSO will request such support in the event of serious system security deficiencies or hazards, or the discovery of a security incident or violation.

(11) Ensure users have the required personnel security clearances, authorizations and need-to-know.

c. The Information System Security Officer (ISSO) will:

(1) Function as the point of contact for all aspects of information security.

(2) Cause operations to be partially or completely suspended upon detection of any action which may affect the security of the operations. This suspension will remain in effect until removed by the CIM or the ISSM.

(3) Ensure implementation of information security by:

(a) Preparing, distributing plans, instructions and guidance, and/or standard operating procedures (SOP) concerning the security of automated information operations.

(b) Conducting periodic surveys or reviews to determine compliance with such regulations.

(c) Conducting reviews of threats and vulnerabilities so as to enable the CIM to properly assess risks and determine effective measures to minimize such risks.

(d) Coordinating any changes in the security environment with the ISSM.

(4) Report immediately to the ISSM any attempt to gain unauthorized access to sensitive defense information or any system failure or suspected defect which could lead to unauthorized disclosure.

(5) Take measures to protect the physical facility.

(6) Review and evaluate the security impact of security changes, including interfaces with other information systems.

(7) Coordinate and monitor periodic security indoctrination and training sessions for assigned personnel.

(8) Compile and maintain the facility security profile (FSP).

(9) Control and manage the issuance of system passwords.

(10) Compile accreditation documentation to accompany the division/office chief's request for accreditation from the appropriate accreditation authority.

(11) Conduct annual training for TASO's and computer users on IM security. Forward training records to the ISSM, stating type of training, names of personnel who attended, and date of training.

(12) Ensure that written instructions are issued specifying security requirements and operating procedures for each terminal area.

(13) Ensure that a TASO is appointed in writing for each terminal or contiguous group of terminals that are not under the direct control of the ISSO.

d. The Network Security Officer (NSO) will:

(1) Ensure that security procedures and protocols governing network operations are developed and issued.

(2) Establish a procedure to control access and connectivity to the network.

(3) Prepare, disseminate, review and maintain plans, instructions, guidance and SOPs concerning security of the network.

(4) Report immediately to the ISSM and ISSO any system failure which could lead to unauthorized disclosure or attempts to gain unauthorized access to sensitive information.

(5) Review and evaluate the security impact of changes to the network, including interfaces with other networks.

(6) Ensure that audit trails and other system management reports are reviewed and used for internal security audits or testing.

e. The Terminal Area Security Officers (TASO) appointed for the remote terminals/microcomputers will:

(1) Ensure that users are familiar with security requirements and operating procedures. Ensure that written instructions specifying security requirements and operating procedures are posted in the computer/terminal areas.

(2) Ensure that each terminal user's identity, need-to-know, level of clearance and access authorizations are coordinated with the ISSM.

(3) Manage and control user or file identification within their element.

(4) Implement controls to prevent entry of unauthorized transactions or data (such as classified data over unsecured data transmission lines) through the remote terminal/microcomputer.

(5) Ensure local compliance with information security procedures.

(6) Report immediately to the ISSO all practices dangerous to system security, and all security violations.

f. The Chief, Information Management (CIM) will:

(1) Review invoices for contract computer services on a monthly basis for visible signs of misuse, e.g., excessive storage usage, exceptionally large charges or noticeable increase in charges.

(2) Audit contract computer services files on an annual basis and maintain a file of the audited reports.

g. Division/Office Chiefs will:

(1) Review and submit accreditation requests and nonsensitive designated analysis to the appropriate accreditation authority through the ISSM.

(2) Ensure fullest consideration of those measures required to provide operational security and protect the integrity of the data and licensed software packages.

(3) Provide in writing a qualified TASO to act as the focal point for security matters for each terminal/microcomputer or clusters of terminal/microcomputers and associated interface devices within that element IAW AR 380-19, para 1-6.d.(5).

(4) Ensure implementation of an effective risk management program IAW AR 380-19, Chap 5.

6. Password Issuance/Control.

a. Mainframe passwords.

(1) Individual users will request issuance of a userid and password on an as needed basis by filling out the userid application form.

(2) The ISSO will enter the request into the Corps of Engineers UPASS system.

(3) The Missouri River Division (MRD) CEAP Family Administrator will validate userid request for access to the CEAP network.

(4) The individual user will sign for the password upon validation. If the user is located outside of the District office the userid and password will be mailed to the individual user.

(5) The ISSO will maintain a current list of authorized users and password.

b. User password control is the responsibility of the individual. The password guideline form issued with the password on it will never be left uncovered or in an obvious location. Users will adhere to all stipulations and requirements of the password guideline.

c. Microcomputers with security packages, e.g., Watchdog or Protec that have userids and passwords will be controlled by the appropriate TASO. Userid will be changed on a semiannual basis and can be user generated. Passwords will be randomly generated by the issuing TASO and will be changed at a minimum of bimonthly. A copy of userids and passwords will be forwarded to the ISSO.

7. Requirements for Security Markings and Disposal of Mainframe-Generated Products.

a. Application programs and output generated from locally developed application programs will have the appropriate sensitivity designation printed on the top of each page of the listing.

b. Printouts that are highly sensitive, e.g., For Official Use Only or Privacy Act will be torn once lengthwise, once width-wise, and disposed of by normal contractor cleaning personnel.

c. Under no circumstances will sensitive printouts be used as personal scratchpads, taken home or given to outside agencies/schools.

8. Accreditation Process Procedures.

a. Accreditation requests will be submitted to the accreditation authority through the ISSM, for all microcomputers, memory typewriters, and any automated information data processing equipment that has memory.

b. Accreditation will consist of the following, at a minimum:

(1) Executive summary.

(2) Accreditation objective.

(3) Risk management review.

(4) Implementation of security controls and countermeasures.

(5) Facility security profile.

(6) Facility floor plan.

(7) Equipment inventory.

(8) Standard operating procedures for security.

c. The accreditation request will be compiled by the ISSO. The ISSM will provide training and assistance.

d. The ISSO of the IM office will provide TASO support for offices with limited IM assets. As a general guideline, if an office has less than four processors, ISSO support will be provided.

e. Reaccreditation will be accomplished IAW AR 380-19, para 3-6.

f. A copy of the accreditation will be kept at the accreditation site and one copy will be retained by the ISSM.

9. Security Training.

a. Division chiefs will be briefed annually by the ISSM on the current IM security plan and their responsibilities.

b. ISSO training will be conducted annually by the ISSM. Training will consist of, at a minimum, issuance of passwords, compilation, review and updates for accreditation requests, and requirements of TASO and user security training.

c. TASO/user training will be conducted on an annual basis by the proponent ISSO. Training will consist of TASO/user responsibilities in the IM security area.

d. Training records will be forwarded to the ISSM.

10. Standards for the Protection of Data, Hardware and Software.

a. All protection of data, hardware and software will comply with AR 380-19, para 2-3.a.(4).

b. Highly sensitive data, sensitive data, and data files that could result in a serious degradation of mission accomplishment should be backed up on either floppy diskette or streamer tape and stored in a locked container physically separate from the computer workstation.

c. Original diskettes of purchased software not copy protected should be kept in a locked container, and backup disks will be used for daily processing.

d. Division/Offices that have large data bases or applications programs, which if destroyed by a localized or catastrophic event could not cost effectively be replaced and would result in the inability to accomplish their mission will contact the CIM to arrange offsite storage IAW DM 25-1-1.

e. Physical security devices for hardware should only be purchased for information data processing equipment that is located in an area not served by security personnel or where theft of equipment is considered a likely possibility.

f. Portable microcomputers should be kept in a locked cabinet when not in use.

11. Waste, Fraud, and Abuse.

a. Microcomputer software licenses are issued to one machine. It is the responsibility of everyone to ensure that license agreements are adhered to. Software cannot be copied for use on more than one machine.

b. Under no circumstances will licensed software be copied for non-official use. Software purchased by the Omaha District is to be used solely for official Corps of Engineers business. All commercial software is protected by copyright laws.

FOR THE COMMANDER:

FOR James Lee Waller LTC, EN
WILLIAM S. PAVLICK
LTC, EN
Deputy Commander

DISTRIBUTION:
B